(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11215122 A**

(43) Date of publication of application: **06.08.99**

(51) Int. Cl **H04L 9/36**
G09C 1/00

(21) Application number: **10013727**

(22) Date of filing: **27.01.98**

(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**

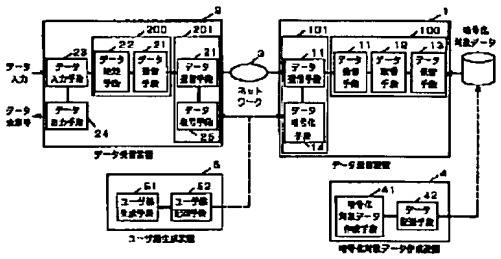
(72) Inventor: **HARADA TOSHIHARU**
OKUMURA YASUO
TATEBAYASHI MAKOTO
SAIJO TAKESHI
ONO TAKATOSHI

(54) **METHOD, DEVICE, AND SYSTEM FOR ENCIPHERING DATA**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method, device, and system for enciphering data by which only the necessary scope of data distributed through WWW(world-wide web) can be enciphered in accordance with the contents of the data.

SOLUTION: (1) A data receiver 2 transmits data request information and receiver identification information when a user inputs data required by the user in a WWW browser 200. (2) A data transmitter 1 enciphers the data to be enciphered corresponding to the data requesting information and incorporating an enciphering scope designating instruction within the extent designated by the enciphering scope designating instruction in such a way that only the receiver can decode the enciphered data in an enciphering proxy 101 and transmits the results to the data receiver 2. (3) The data receiver 2 decodes the enciphered data in a decoding proxy 201 and outputs the decoded data.



(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－215122

(43)公開日　平成11年(1999)8月6日

(51)Int.Cl.⁶		識別記号	FI		
H04L	9/36		H04L	9/00	685
G09C	1/00	660	G09C	1/00	660Z

審査請求　未請求　請求項の数15　OL　（全19頁）

(21)出願番号　特願平10－13727

(22)出願日　平成10年(1998)1月27日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　奥村　康男
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　滝本　智之　（外1名）

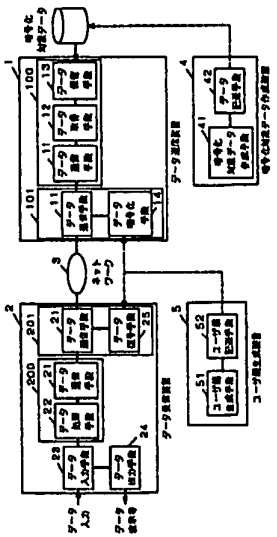
最終頁に続く

(54)【発明の名称】　データ暗号方法、データ暗号装置、及びデータ暗号システム

(57)【要約】

【課題】　WWWで配信されるデータに対して、その内容に応じて必要な範囲だけを暗号化する方法、装置及びシステムを提供する。

【解決手段】　(1)データ受信装置2は、WWWブラウザ200において、ユーザから取得したいデータの入力を受けとると、データ要求情報と受信者識別情報を送信する。(2)データ送信装置1は、暗号プロキシ101において、データ要求情報に対応した、暗号化範囲指定命令が組み込まれた暗号化対象データに対して、暗号化範囲指定命令で指定された範囲を、受信者識別情報で指定された受信者のみが復号できるように暗号化しこの結果をデータ受信装置2に送信する。(3)データ受信装置2は、復号プロキシ201において暗号化された暗号化対象データを復号し、復号されたデータを出力する。



【特許請求の範囲】

【請求項1】暗号化処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行なうデータ暗号方法であって、
暗号化する範囲を指定する暗号化範囲指定命令が組み込まれた暗号化対象データに対して、前記暗号化範囲指定命令で指定された範囲を暗号化することを特徴とするデータ暗号方法。

【請求項2】前記暗号化対象データに、前記暗号化範囲指定命令に加えて、前記暗号化対象データの受信者を指定する受信者指定命令が組み込まれている場合に、
前記受信者指定命令で指定された受信者が保持する復号鍵に対応する暗号化鍵を用いて、前記暗号化対象データのうち、前記暗号化範囲指定命令により指定された範囲を暗号化するようにしたことを特徴とする請求項1記載のデータ暗号方法。

【請求項3】前記暗号化対象データを暗号化するに際し、前記暗号化対象データを第1の暗号化鍵で暗号化し、前記第1の暗号化鍵に対応する第1の復号鍵を、受信者の保持する第2の復号鍵に対応する第2の暗号化鍵で暗号化し、暗号化された前記暗号化対象データに、暗号化された前記第1の復号鍵を指定する鍵情報指定命令を組み込んだ暗号化データを得るようにしたことを特徴とする請求項1記載のデータ暗号方法。

【請求項4】復号処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行なうデータ暗号方法であって、
復号する範囲を指定する復号範囲指定命令が組み込まれた暗号化データに対して、前記復号範囲指定命令で指定された範囲を復号することを特徴とするデータ暗号方法。

【請求項5】前記暗号化データに、前記復号範囲指定命令に加えて、暗号化データの受信者を指定する受信者指定命令が組み込まれている場合に、
前記受信者指定命令で指定された受信者が保持する復号鍵を用いて、前記暗号化データに対して、前記復号範囲指定命令により指定された範囲を前記復号鍵を用いて復号するようにしたことを特徴とする請求項4記載のデータ暗号方法。

【請求項6】前記暗号化データに、前記復号範囲指定命令に加えて、暗号化された前記第1の復号鍵を指定する鍵情報指定命令が組み込まれている場合に、
前記暗号化データを復号するに際し、前記鍵情報指定命令で指定された暗号化された前記第1の復号鍵を、受信者の保持する第2の復号鍵で、復号し、
前記暗号化データを、復号された前記第1の復号鍵で、前記復号範囲指定命令により指定された範囲を前記復号鍵を用いて復号するようにしたことを特徴とする請求項4記載のデータ暗号方法。

【請求項7】前記暗号化対象データに組み込まれる命令が、特に、HTML (Hypertext Markup Language) 言語に基づいた命令である場合に、暗号処理のための命令群、すなわち前記暗号化範囲指定命令、前記復号範囲指定命令、前記受信者指定命令、及び、前記鍵情報指定命令の記述方法として、前記HTMLで定義されているコメント指定用の命令を利用し、そのコメントとしてあらかじめ定めた特定のコメントが指定された時に前述の暗号処理のための命令群の中から対応する命令が指定されたものとみなすようにしたことを特徴とする請求項1から6のうちいずれか1項記載のデータ暗号方法。

【請求項8】暗号化処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行なうデータ暗号装置であって、データ通信手段と、データ取得手段と、データ保管手段と、データ暗号化手段を備え、
前記データ通信手段が、前記データ保管手段に保管された暗号化対象データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化対象データを前記データ保管手段から取得し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、データ通信手段が、前記暗号化データを前記データ要求情報の発信元に送信することを特徴とするデータ暗号装置。

【請求項9】前記データ暗号装置が、特に、前記データ通信手段と、前記データ取得手段と、前記データ保管手段を備えたWWW(World Wide Web)サーバと、前記データ暗号化手段を有する暗号化プログラムとが実装されたコンピュータであることを特徴とする請求項8記載のデータ暗号装置。

【請求項10】前記暗号化プログラムが、前記データ暗号化手段に加えて、WWWサーバまたはWWWブラウザと、前記暗号化対象データもしくは前記暗号化データの送受信を行うためのデータ通信手段を有するプログラムであることを特徴とする請求項9記載のデータ暗号装置。

【請求項11】復号処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行なうデータ暗号装置であって、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段を備え、
前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化対象データの送信を要求するデー

タ要求情報を送信し、前記データ要求情報に対応する、復号する範囲を指定する復号範囲指定命令が組み込まれた暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号装置。

【請求項12】前記データ受信装置が、特に、前記データ通信手段と、前記データ処理手段と、前記データ入力手段と、前記データ出力手段を備えたWWWブラウザと、前記データ復号手段を有する復号プログラムが実装されたコンピュータであることを特徴とする請求項11記載のデータ暗号装置。

【請求項13】前記復号プログラムが、前記データ復号手段に加えて、WWWサーバまたはWWWブラウザと、前記暗号化対象データもしくは前記暗号化データの送受信を行うためのデータ通信手段を有するプログラムであることを特徴とする請求項12記載のデータ暗号装置。

【請求項14】データ通信手段と、データ取得手段と、データ保管手段と、データ暗号化手段と、ユーザ鍵保管手段とを備えた送信側のデータ暗号装置と、
データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段と、ユーザ鍵保管手段とを備えた受信側のデータ暗号装置と、
ネットワークと、暗号化対象データ作成手段と暗号化対象データ配送手段を備えた暗号化対象データ作成装置と、
ユーザ鍵生成手段とユーザ鍵配送手段を備えたユーザ鍵生成装置とで構成されるデータ暗号システムであって、
前記ユーザ鍵生成装置において、前記ユーザ鍵生成手段が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前記ユーザ鍵配送手段が、前記暗号化鍵を前記送信側のデータ暗号装置のユーザ鍵保管手段に保管し、前記復号鍵を前記受信側のデータ暗号装置のユーザ鍵保管手段に保管し、
前記暗号化対象データ作成装置において、前記暗号化対象データ作成手段が、暗号化する範囲を指定する暗号化範囲指定命令を組み込んだ暗号化対象データを作成し、前記暗号化対象データ配送手段が、前記暗号化対象データを前記送信側のデータ暗号装置のデータ保管手段に保管し、
前記受信側のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化対象データの送信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送信し、
前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ保管手段に保管された暗号化対象データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化対象データを前記データ保管手段から取得し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、データ通信手段が、前記暗号化データを前記受信側のデータ暗号装置に前記ネットワークを利用して送信し、
前記受信側のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号システム。

【請求項15】データ通信手段と、データ取得手段と、データ保管手段とを備えた送信側のデータ暗号装置と、
データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段と、ユーザ鍵保管手段とを備えた受信側のデータ暗号装置と、ネットワークと、
暗号化対象データ作成手段と、データ暗号化手段と、ユーザ鍵保管手段と、暗号化データ配送手段を備えた暗号化データ作成装置と、
ユーザ鍵生成手段とユーザ鍵配送手段を備えたユーザ鍵生成装置とで構成されるデータ暗号システムであって、
前記ユーザ鍵生成装置において、前記ユーザ鍵生成手段が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前記ユーザ鍵配送手段が、前記暗号化鍵を前記暗号化データ作成装置のユーザ鍵保管手段に保管し、前記復号鍵を前記受信側のデータ暗号装置のユーザ鍵保管手段に保管し、
前記暗号化データ作成装置において、前記暗号化データ作成手段が、暗号化する範囲を指定する暗号化範囲指定命令を組み込んだ暗号化対象データを作成し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、前記暗号化データ配送手段が、前記暗号化データを前記送信側のデータ暗号装置のデータ保管手段に保管し、
前記受信側のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化データの送信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送信し、
前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ保管手段に保管された暗号化データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化データを前記データ保管手段から取得し、データ通信手段が、前記暗号化データを前記受信側のデータ暗号装置に前記ネットワークを利用して送信し、
前記受信側のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力することを特徴とするデータ暗号システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】暗号処理命令を含むデータ処理命令の組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号処理を施すための方法、装置、及びシステムに関する。

【0002】

【従来の技術】WWW(World Wide Web)システムは、マルチメディア情報の検索や、不特定多数への情報発信といった機能を、非常に簡便なユーザインターフェースで提供するため急速に普及している。このため、WWWシステムを、パソコンソフトのオンライン販売など、商用システムを構築する際のプラットフォームとして利用されつつある。

【0003】WWWシステムを利用して発信される有料の電子情報や、部外秘の電子情報（以下、単にWWWデータと称する）を、特定の受信者以外に盗聴（盗見）されないようにするために、WWWデータを暗号化することが考えられる。また、特に商用利用の場合は、WWWデータを、その内容に応じて、一部を視聴可能とし、重要な部分だけを暗号化するといった、きめ細かく暗号化することが考えられる。

【0004】従来、WWWシステムで発信する電子情報を暗号化する方法としては、NetscapeCommunications社が提唱するSSL(Secure Socket Layer)やEnterprise Integration Technologies社が提唱するS-HTTPがあり、これらを用いるとWWWデータは暗号化されるため第三者への盗聴（盗見）を防止することができる。なお、SSL及びS-HTTPについては、例えば、CQ出版社のOPEN DESIGN、1996年6月号（第7章）を参照されたい。

【0005】

【発明が解決しようとする課題】しかしながら、これらの従来方法は、いずれも、WWWデータを発信するWWWサーバと、WWWデータを受信するWWWブラウザ間で伝送されるWWWデータ全体に対して一律的に暗号化するものであった。このため、WWWデータの内容に応じて、一部はすべての受信者に視聴を可能とし、重要な部分だけを暗号化するといった、きめ細かな暗号化が行えなかった。また、従来方法では、上述のSSLまたはS-HTTPに基づく暗号機能が追加された専用のWWWサーバ及びWWWブラウザが必要であった。そして、例えば、SSLに基づく暗号機能が追加されたWWWサーバは、SSLに基づく暗号機能が追加されたWWWブラウザとの間でのみ、WWWデータの暗号通信が可能であった。

【0006】本発明は、上記従来の問題点に鑑み、WWWデータを暗号化するに際し、データの内容に応じて、必要な範囲だけを暗号化でき、また、必要であればあらかじめ指定した受信者のみが復号できるようにWWWデータを暗号化することも可能とする、データの暗号方法、装置及びシステムを提供することを第1の目的とする。

【0007】また、既存のWWWサーバやWWWブラウザに暗号機能を追加する必要のない、すなわち、本発明のデータ暗号化方法に基づく暗号機能が追加された専用のWWWサーバやWWWブラウザを必要としない、データの暗号化方法、復号方法、暗号通信方法、及び、その装置及びシステムを提供することを第2の目的とする。

【0008】

【課題を解決するための手段】上記目的を達成するために、本発明は、暗号化処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行なうデータ暗号方法であって、暗号化する範囲を指定する暗号化範囲指定命令が組み込まれた暗号化対象データに対して、前記暗号化範囲指定命令で指定された範囲を暗号化する手段を備える。

【0009】また、前記暗号化対象データに、前記暗号化範囲指定命令に加えて、前記暗号化対象データの受信者を指定する受信者指定命令が組み込まれている場合に、前記受信者指定命令で指定された受信者が保持する復号鍵に対応する暗号化鍵を用いて、前記暗号化対象データのうち、前記暗号化範囲指定命令により指定された範囲を暗号化する手段を備える。

【0010】また、前記暗号化対象データを暗号化するに際し、前記暗号化対象データを第1の暗号化鍵で暗号化し、前記第1の暗号化鍵に対応する第1の復号鍵を、受信者の保持する第2の復号鍵に対応する第2の暗号化鍵で暗号化し、暗号化された前記暗号化対象データに、暗号化された前記第1の復号鍵を指定する鍵情報指定命令を組み込んだ暗号化データを得る手段を備える。

【0011】また、復号処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行なうデータ暗号方法であって、復号する範囲を指定する復号範囲指定命令が組み込まれた暗号化データに対して、前記復号範囲指定命令で指定された範囲を復号する

手段を備える。

【0012】また、前記暗号化データに、前記復号範囲指定命令に加えて、暗号化データの受信者を指定する受信者指定命令が組み込まれている場合に、前記受信者指定命令で指定された受信者が保持する復号鍵を用いて、前記暗号化データに対して、前記復号範囲指定命令により指定された範囲を前記復号鍵を用いて復号する手段を備える。

【0013】また、前記暗号化データに、前記復号範囲指定命令に加えて、暗号化された前記第1の復号鍵を指定する鍵情報指定命令が組み込まれている場合に、前記暗号化データを復号するに際し、前記鍵情報指定命令で指定された暗号化された前記第1の復号鍵を、受信者の保持する第2の復号鍵で、復号し、前記暗号化データを、復号された前記第1の復号鍵で、前記復号範囲指定命令により指定された範囲を前記復号鍵を用いて復号する手段を備える。

【0014】また、前記暗号化対象データに組み込まれる命令が、特に、HTML(Hypertext Markup Language)言語に基づいた命令である場合に、暗号処理のための命令群、すなわち前記暗号化範囲指定命令、前記復号範囲指定命令、前記受信者指定命令、及び、前記鍵情報指定命令の記述方法として、前記HTMLで定義されているコメント指定用の命令を利用し、そのコメントとしてあらかじめ定めた特定のコメントが指定された時に前述の暗号処理のための命令群の中から対応する命令が指定されたものとみなすようにする。

【0015】また、暗号化処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化対象データに対して、組み込まれた命令に従って暗号化処理を含むデータ処理を行なうデータ暗号装置であって、データ通信手段と、データ取得手段と、データ保管手段と、データ暗号化手段を備え、前記データ通信手段が、前記データ保管手段に保管された暗号化対象データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化対象データを前記データ保管手段から取得し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、データ通信手段が、前記暗号化データを前記データ要求情報の発信元に送信する。

【0016】また、前記データ暗号装置が、特に、前記データ通信手段と、前記データ取得手段と、前記データ保管手段を備えたWWW(World Wide Web)サーバと、前記データ暗号化手段を有する暗号化プログラムとが実装されたコンピュータである。

【0017】また、前記暗号化プログラムが、前記データ暗号化手段に加えて、WWWサーバまたはWWWブラウザと、前記暗号化対象データもしくは前記暗号化データの送受信を行うためのデータ通信手段を有するプログラムである。

【0018】また、復号処理方法を含むデータ処理方法を指定する命令が組み込まれた暗号化データに対して、組み込まれた命令に従って復号処理を含むデータ処理を行なうデータ暗号装置であって、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段を備え、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記データ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送信し、前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ要求情報に対応する、復号する範囲を指定する復号範囲指定命令が組み込まれた暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力する。

【0019】また、前記データ受信装置が、特に、前記データ通信手段と、前記データ処理手段と、前記データ入力手段と、前記データ出力手段を備えたWWWブラウザと、前記データ復号手段を有する復号プログラムが実装されたコンピュータである。

【0020】また、前記復号プログラムが、前記データ復号手段に加えて、WWWサーバまたはWWWブラウザと、前記暗号化対象データもしくは前記暗号化データの送受信を行うためのデータ通信手段を有するプログラムである。

【0021】また、データ通信手段と、データ取得手段と、データ保管手段と、データ暗号化手段と、ユーザ鍵保管手段とを備えた送信側のデータ暗号装置と、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段と、ユーザ鍵保管手段とを備えた受信側のデータ暗号装置と、ネットワークと、暗号化対象データ作成手段と暗号化対象データ配送手段を備えた暗号化対象データ作成装置と、ユーザ鍵生成手段とユーザ鍵配送手段を備えたユーザ鍵生成装置とで構成されるデータ暗号システムであって、前記ユーザ鍵生成装置において、前記ユーザ鍵生成手段が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前記ユーザ鍵配送手段が、前記暗号化鍵を前記送信側のデータ暗号装置のユーザ鍵保管手段に保管し、前記復号鍵を前記受信側のデータ暗号装置のユーザ鍵保管手段に保管し、前記暗号化対象データ作成装置において、前記暗号化対象データ作成手段が、暗号化する範囲を指定する暗号化範囲指定命令を組み込んだ暗号化対象データを作成し、前記暗号化対象データ配送手段が、前記暗号化対象データを前記送信側のデータ暗号装置のデータ保管手段に保管し、前記受信側のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化対象データの送信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送信し、前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ保管手段に保管された暗号化対象データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化対象データを前記データ保管手段から取得し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、データ通信手段が、前記暗号化データを前記受信側のデータ暗号装置に前記ネットワークを利用して送信し、前記受信側のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力する。

【0022】また、データ通信手段と、データ取得手段と、データ保管手段とを備えた送信側のデータ暗号装置と、データ通信手段と、データ処理手段と、データ入力手段と、データ出力手段と、データ復号手段と、ユーザ鍵保管手段とを備えた受信側のデータ暗号装置と、ネットワークと、暗号化対象データ作成手段と、データ暗号化手段と、ユーザ鍵保管手段と、暗号化データ配送手段を備えた暗号化データ作成装置と、ユーザ鍵生成手段とユーザ鍵配送手段を備えたユーザ鍵生成装置とで構成されるデータ暗号システムであって、前記ユーザ鍵生成装置において、前記ユーザ鍵生成手段が、各ユーザ固有の暗号化鍵とこの暗号化鍵に対応する復号鍵を生成し、前記ユーザ鍵配送手段が、前記暗号化鍵を前記暗号化データ作成装置のユーザ鍵保管手段に保管し、前記復号鍵を前記受信側のデータ暗号装置のユーザ鍵保管手段に保管し、前記暗号化データ作成装置において、前記暗号化データ作成手段が、暗号化する範囲を指定する暗号化範囲指定命令を組み込んだ暗号化対象データを作成し、前記データ暗号化手段が、前記暗号化対象データのうち前記暗号化範囲指定命令により指定された範囲を暗号化し、この結果として得られる少なくとも一部が暗号化された前記暗号化対象データに、復号する範囲を指定する復号範囲指定命令を組み込んだ暗号化データを作成し、前記暗号化データ配送手段が、前記暗号化データを前記送信側のデータ暗号装置のデータ保管手段に保管し、前記受信側のデータ暗号装置において、前記データ入力手段に、外部から取得したい暗号化対象データを指定する情報が入力されたとき、前記データ通信手段が、前記暗号化データの送信を要求するデータ要求情報を前記送信側のデータ暗号装置に前記ネットワークを利用して送信し、前記送信側のデータ暗号装置において、前記データ通信手段が、前記データ保管手段に保管された暗号化データの送信を要求するデータ要求情報を受信したとき、前記データ取得手段が、前記データ要求情報で要求された前記暗号化データを前記データ保管手段から取得し、データ通信手段が、前記暗号化データを前記受信側のデータ暗号装置に前記ネットワークを利用して送信し、前記受信側のデータ暗号装置において、前記暗号化データを受信し、前記データ復号手段が、前記暗号化データのうち復号範囲指定命令で指定された範囲を復号し、前記データ処理手段が、復号された暗号化データを、ディスプレやプリンタなどのデータ出力装置が接続された前記データ出力手段に出力する。

【0023】

【発明の実施の形態】以下に、本発明の実施の形態について、図面を用いて説明する。なお、本実施の形態では、データを送信するデータ送信装置として、WWWサーバを利用し、また、データを受信するデータ受信装置として、WWWブラウザを利用する場合について説明する。

【0024】また、送信されるデータは、WWWサーバで配信されるデータの標準的な記述言語であるHTML(Hypertext Markup Language)言語に基づいて、各種データ処理命令が組み込まれる場合について説明する。

【0025】また、データの暗号化には、DES(Data Encryption Standard)暗号方式等の共通鍵暗号方式を利用し、データの暗号化に利用した暗号化鍵（以下、データ鍵と称する）の暗号化には、RSA暗号方式等の公開鍵暗号方式を利用する場合について説明する。DES暗号方式およびRSA暗号方式については、例えば岡本英司著、「暗号理論入門」共立出版（第3章及び第5章）を参照されたい。

【0026】（実施の形態1）まず、データ送信装置にあらかじめ暗号化対象データ（暗号化されていない平文のデータ）を格納しておき、データ送信装置にて、データ受信装置からの送信要求に対応して、該当の暗号化対象データを暗号化し、得られた暗号化データをデータ受信装置に送信し、データ受信装置にて、受信した暗号化データを復号して取得する場合について説明する。

【0027】まず、システム構成について説明し、次に、本システムで扱うデータの構造について説明する。そして、本システムの動作詳細について説明する。

【0028】「システムの構成」本実施の形態の全体のシステム構成の概略について説明する。図1は、本実施の形態におけるデータ暗号通信システムの概略構成図である。図1に示すようにデータ暗号通信システムは、データ送信装置1と、データ受信装置2と、これらを接続

するネットワーク３と、暗号化対象データ作成装置４と、ユーザ鍵生成装置５によって構成される。

【００２９】データ送信装置１は、データ受信装置２からのデータ要求情報及びオプションとして受信者識別情報を受信しそのデータ要求情報に対応した暗号化データをデータ受信装置２に送信するためのデータ通信手段１１と、上記データ要求情報に対応する暗号化対象データをデータ保管手段１３から取り出し、この暗号化対象データをデータ暗号化手段１４に渡し、その結果として生成される暗号化データを取得し、この暗号化データをデータ通信手段に渡すためのデータ取得手段１２と、暗号化対象データを保管するデータ保管手段１３と、暗号化対象データを受信者識別情報もしくは後で述べる受信者指定命令にて指定された受信者向けに暗号化して暗号化データを生成するためのデータ暗号化手段１４を備えている。データ暗号化手段には、図示していないがユーザ鍵生成装置５によって生成された各ユーザのユーザ公開鍵を保管するための公開鍵保管手段を備えている。データ暗号化手段１４の詳細構成については後で説明する。

【００３０】データ送信装置１としては、具体的には、上記データ通信手段と、データ取得手段と、データ保管手段を備えた、既存のWWW(World Wide Web)サーバ（例えば、Netscape Communications社のNetscape Communicationサーバなど）を実装したコンピュータ（パソコンやワークステーションなど）が利用できる。この場合、WWWサーバの備えるデータ通信手段１１が、WWWサーバとWWWブラウザ間の標準通信プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

【００３１】データ送信装置におけるデータ暗号化手段１４の実現方法としては、具体的には、CGI（Common Gateway Interface）プログラム（各種データ処理機能をWWWサーバに追加するためのプログラム）を利用できる。データ送信装置１を、WWWサーバとCGIプログラムで実現する場合の構成図を図２（１）に示す。図２（１）に示すように、CGIプログラムを利用する場合は、データ送信装置は、データ暗号化手段を提供するCGIプログラム１０１が組み込まれたWWWサーバ１００で構成され、CGIプログラム１０１とWWWサーバ１００は一体のプログラムとして動作する。すなわち、CGIプログラムを利用する場合、WWWサーバ毎にCGIプログラムを追加する必要がある。

【００３２】なお、データ送信装置におけるデータ暗号化手段１４の別の実現方法として、暗号化処理代行プログラム（以下、暗号化プロキシと称する）を利用することもできる。暗号化プロキシで実現する場合のデータ送信装置の構成図を図２（２）に示す。

【００３３】また、図３に、データ送信装置をWWWサーバと暗号化プロキシで構成した場合のシステムの全体構成を示す。

【００３４】図２（２）及び図３に示すように、暗号化プロキシによる構成を利用する場合は、データ送信装置１は、WWWサーバ１００と、データ暗号化手段１４とデータ通信手段１５を備えた暗号化プロキシ１０２で構成される。

【００３５】ここで暗号化プロキシ１０２におけるデータ通信手段１５は、WWWサーバとWWWブラウザ間のデータ通信のための標準プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

【００３６】この構成により、WWWサーバ１００と暗号化プロキシ１０２は、それぞれ独立のプログラムとして動作させることが可能となる。そして、その結果、WWWサーバとして既存のWWWサーバをそのまま利用することができ、また、複数のWWWサーバに一つの暗号化プロキシでデータ暗号化手段を追加することも可能となる。

【００３７】また、データ受信装置２は、データ送信装置１にデータ要求情報及びオプションとして受信者識別情報を送信し、そのデータ要求情報に対応した暗号化データを受信するためのデータ通信手段２１と、受信した暗号化データをデータ復号手段に渡し、その結果として得られる復号された暗号化データに対して、各種データ処理（例えばデータの表示、データの保存、データの印刷などの処理）を施すためのデータ処理手段２２と、暗号化データを復号して、復号された暗号化データを生成するためのデータ復号手段２３と、ユーザから各種データ処理の指定（例えば取得したいデータの指定、データの保存やデータの印刷などの処理の指定など）を受けるためのデータ入力手段２３と、データの表示やデータの印刷などのためにディスプレやプリンタなどの外部装置にデータを出力するためのデータ出力手段２４を備えている。

【００３８】データ復号手段には、図示していないが鍵生成装置５によって生成されたユーザ秘密鍵（このデータ受信装置を利用するユーザのユーザ秘密鍵）を保管するための公開鍵保管手段を備えている。データ復号手段２５の詳細構成については後で説明する。

【００３９】データ受信装置２としては、具体的には、上記データ通信手段と、データ処処理手段を備えた既存のWWWブラウザ（例えば、Netscape Communications社Netscape Navigatorや、Microsoft社のInternet Explorer）を実装したコンピュータ（パソコンやワークステーションなど）が利用できる。この場合、WWWブラウザの備えるデータ通信手段２１が、WWWサーバとWWWブラウザ間の標準通信プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。また、データ入力手段としては、上記コンピュータの備えるキーボードやマウス等を利用できる。またデータ出力手段にはディスプレやプリンタ等が接続されている。

【００４０】データ受信装置２におけるデータ復号手段２５の実現手段としては、具体的には、WWWブラウザのプラグイン（各種データ処理機能をWWWブラウザに追加するためのプログラム）を利用することができる。データ復号手段を、プラグインで実現する場合のデータ復号手段の構成図を図２（３）に示す。図２（３）に示すように、プラグインを利用する場合は、データ受信装置は、データ復号手段を提供する復号プラグイン２０１が組み込まれたWWWブラウザ２００で構成され、WWWブラウザと復号プラグインは一体のプログラムとして動作する。

【００４１】すなわち、プラグインを利用する場合、WWWブラウザ毎にプラグインを追加する必要がある。

【００４２】なお、データ受信装置におけるデータ復号手段１４の別の実現方法として、復号処理代行プログラム（以下、復号プロキシと称する）を利用することもできる。復号プロキシで実現する場合のデータ受信装置の構成図を図２（４）に示す。また、図3に、データ受信装置をWWWブラウザと復号プロキシで構成した場合のシステムの全体構成を示す。

【００４３】図２（４）及び図３に示すように、復号プロキシによる構成を採用する場合は、データ受信装置２は、WWWブラウザ２００と、データ復号手段２３に加えてデータ通信手段２１を備えた復号プロキシ２０２で構成される。

【００４４】ここで復号プロキシ２０２におけるデータ通信手段は、WWWサーバとWWWブラウザ間のデータ通信のための標準プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

【００４５】この構成により、WWWブラウザ２００と復号プロキシ２０２は、それぞれ独立のプログラムとして動作させることが可能となる。そして、その結果、WWWブラウザとして既存のWWWブラウザがそのまま利用でき、また、複数のWWWブラウザに一つの復号プロキシでデータ復号手段を追加することも可能となる。

【００４６】暗号化対象データ作成装置４としては、暗号化対象データを作成する暗号化対象データ作成手段４１と、作成した暗号化対象データをデータ送信装置１のデータ保管手段１３に配送するデータ配送手段４２が備えられている。

【００４７】暗号化対象データ作成装置４として、具体的には、通常のテキストエディターや既存のWWWデータ（ホームページなど）を作成するための市販のソフトウエアが実装されたコンピュータ（パソコンやワークステーション）が利用できる。またデータ配送手段４２の具体的な実現方法としては、例えば、暗号化対象データをフロッピーディスクなどの記録媒体に記録してオフラインで配送する手段等をとることができる。

【００４８】暗号化対象データのデータ構造については、後で説明する。ユーザ鍵生成装置５は、各ユーザ毎に固有のユーザ秘密鍵及びユーザ公開鍵を生成するユーザ鍵生成手段５１と、生成したユーザ秘密鍵をデータ受信装置の秘密鍵保管手段に配送するとともに、生成したユーザ公開鍵を、データ暗号化装置の公開鍵保管手段に配送するためのユーザ鍵配送手段５２を備えている。ユーザ鍵生成装置５としては、具体的には、ユーザ鍵生成プログラムを実装したパソコンやワークステーションなどが利用できる。またユーザ秘密鍵を配送するためのユーザ鍵配送手段としては、例えば、ICカードなどの物理的に安全な媒体に記録してオフラインで配送する手段や、ユーザ秘密鍵をユーザのパスワード等を用いて共通鍵暗号方式により暗号化した上でフロッピーディスク等の記録媒体に記録して配送する手段や、パスワード等で暗号化されたユーザ秘密鍵をネットワークを利用して配送する手段などを利用することができる。また、ユーザ公開鍵を配送するためのユーザ鍵配送手段としては、例えば、ICカードなどの物理的に安全な媒体に記録して配送する手段や、認証局と呼ばれる公的機関にユーザ公開鍵に対する証明書の発行を受けた上で、ユーザ公開鍵と証明書を、フロッピーディスクなどの記録媒体に記録してオフラインで配送する手段や、または、ユーザ公開鍵と証明書をネットワークを利用してオンラインで電子的に配送する手段などを利用することができる。

【００４９】なお、ここでは、データ送信装置１、データ受信装置２、暗号化対象データ作成装置４、ユーザ鍵生成装置５は、それぞれ異なる装置として実現する場合について説明したが、これらの装置を同じコンピュータで実現することも可能である。例えば、ユーザの利用するコンピュータに、暗号化対象データ作成装置と、データ受信装置と、ユーザ鍵生成装置の各機能を持たせる構成も可能である。

【００５０】「暗号対象データ及び暗号化データの構造」次に、本実施の形態で扱う、暗号処理を含むデータ処理命令が組み込まれた暗号化対象データと、この暗号対象データを組み込まれた命令に従って暗号化した結果として得られる暗号化データのデータ構造について説明する。

【００５１】なお、ここでは、暗号化対象データおよび暗号化データとして、WWWデータの標準的な記述言語である、HTML（Hypertext Markup Language）言語に基づいて作成する場合について説明するが、他の記述言語に基づいて同様に作成することも可能である。

【００５２】図５（１）は、本実施の形態で扱う暗号化対象データの構造例である。図５（１）に示すように、暗号化対象データD1は、通常のHTML言語で記述されたデータ本体D0に、暗号化するデータ範囲を指定する暗号化範囲指定命令C1や、この暗号化対象データの受信者を指定する受信者指定命令C2などの暗号処理命令群が追加された構造をとる。

【００５３】また、図５（２）は、本実施の形態で扱う暗号化データの構造例である。図５（２）に示すように、暗号化データD2は、復号する範囲を指定する復号範囲指定命令C3や、この暗号化データの受信者が復号す

る際に利用する鍵情報を指定するための鍵情報指定命令C4などの暗号処理命令群が追加された構造をとる。

【0054】図6に、暗号対象データ及び暗号化データに組み込まれる暗号処理命令群の例について示す。図6において、暗号化範囲指定命令は、暗号化対象データにおいて必ず指定される命令であり、暗号化対象データのうち暗号化する範囲を指定する命令である。暗号化範囲指定命令により、データ提供者は、提供するデータに対して、必要に応じて、必要な範囲だけを暗号化して提供することが可能となる。

【0055】また、受信者指定命令は、必要に応じて指定される命令であり、暗号化対象データを受信する受信者をあらかじめ指定する命令である。受信者指定命令が指定された場合、データ暗号化装置のデータ暗号化手段は、この受信者指定命令により指定された受信者のみが正しく復号できるように暗号化対象データを暗号化する。データの暗号化の詳細構成については後で説明する。

【0056】データ提供者は、受信者指定命令を利用することにより、あらかじめ指定した受信者以外には、提供するデータが、復号できないように制御することが可能となる。

【0057】また、暗号化範囲指定命令は、具体的には、次のような文字列<!--BEGIN SECRET->と、<!--END SECRET->で暗号化範囲の開始と終了を指定し、これらで囲まれたデータを暗号化することを指定する。なお、ここで、HTML言語では、文字列"<!＊＊＊-->は、通常の命令とは異なり単なるコメントとして扱われる（以下、この命令をコメント命令と称する）。したがって、既存のWWWブラウザや、WWWサーバにおいて、暗号化範囲指定命令は、コメントとして無視され、WWWブラウザや、WWWサーバに影響を及ぼすことはない。同様に、図9に示すように他の暗号処理命令も、HTML言語のコメント命令を利用し、それぞれ特定の文字列を所定の暗号処理命令に割り当てている。このようにコメント命令を利用することにより、既存のWWWサーバやブラウザに影響を与えることなく、データを必要に応じて必要な範囲のみを暗号化したり、指定した受信のみが復号できるように暗号化するための命令を暗号化対象データに組み込むことが可能となる。

【0058】「データ暗号化手段及びデータ復号手段の詳細構成」ここでは、データ送信装置1におけるデータ暗号化手段14と、データ受信装置2におけるデータ復号手段25の詳細構成について説明する。

【0059】まず、データ暗号化手段14の詳細構成を図4に示す。図4に示すように、データ暗号化手段14は、暗号化対象データを暗号化する際に利用する、乱数であるデータ鍵を生成するためのデータ鍵生成手段141と、データ鍵生成手段141にて生成されたデータ鍵を用いて、共通鍵暗号方式により暗号化対象データのうち暗号化範囲指定命令で指定された範囲を暗号化する共通鍵暗号化手段142と、各ユーザのユーザ公開鍵を保管するユーザ公開鍵保管手段143と、ユーザ公開鍵保管手段143において保管されているユーザ公開鍵の中から、受信者指定命令、もしくは、データ受信装置から受信した受信者識別情報により指定された受信者のユーザ公開鍵を取り出し、取り出されたユーザ公開鍵を用いて、公開鍵暗号方式により、データ鍵を暗号化する公開鍵暗号化手段144と、暗号化された暗号化対象データに、復号する範囲を指定する復号範囲指定命令や、暗号化されたデータ鍵を指定する鍵情報指定命令を追加する暗号化データ生成手段145より構成される。

【0060】データ復号手段13の詳細構成を図4（2）に示す。図4（2）に示すように、データ復号手段25は、暗号化データから鍵情報指定命令で指定された暗号化されたデータ鍵を取り出し、この暗号化されたデータ鍵を公開鍵復号手段253に渡し、暗号化データのうち復号範囲指定命令で指定された範囲を共通鍵復号手段254に渡すための暗号化データ解析手段251と、ユーザ秘密鍵を保管する秘密鍵保管手段252と、秘密鍵保管手段252において管理されているユーザ秘密鍵を用いて、暗号化されたデータ鍵を、データ暗号化手段において利用したものと同じ公開鍵暗号方式を用いて復号する公開鍵復号手段253と、復号されたデータ鍵を用いて、データ暗号化手段において利用したものと同じ共通鍵暗号方式を用いて、暗号化データのうち復号範囲指定命令で指定された範囲を復号する共通鍵復号手段254より構成される。

【0061】「詳細な動作」次に、本実施の形態の動作について説明する。

【0062】まず、全体の動作概略について説明し、その後、個々の処理の詳細動作について説明する。

【0063】（1） 本実施の形態全体の動作概略

図7は、本実施の形態におけるデータ暗号通信システムの全体の動作概略を示すフローチャートである。

【0064】図7に示すように、本実施の形態は、新規のユーザが利用を開始するときに行うユーザ鍵生成処理（ステップS100）と、データの提供者が提供データ（暗号化対象データ）を作成するときに行うデータ作成処理（ステップS200）と、ユーザが、提供データを取得するときに行うデータ取得処理（ステップS300）からなる。

【0065】ここでユーザ鍵生成処理（S100）は、ユーザ自身、もしくは、本システムの管理者が、ユーザ鍵生成装置を利用して行う。具体的には、各ユーザ用のユーザ秘密鍵と、ユーザ秘密鍵に対応するユーザ公開鍵を生成し、生成したユーザ秘密鍵をそのユーザの利用するデータ受信装置に、またユーザ公開鍵を、データ送信装置に配送するなどの処理を行う。

【0066】データ作成処理（S200）は、データ提供者が、暗号化対象データ作成装置を利用して行う。具体的には、暗号化対象データを作成し、作成した暗号化対象データを、データ送信装置に配送するなどの処理を行う。

【0067】データ取得処理（S300）は、各ユーザが、データ受信装置を利用して行う。具体的には、各ユーザが、自分のデータ受信装置を利用して、取得したい提供データ（暗号化対象データ）の送信を要求するデータ要求情報をデータ送信装置に送信し、データ送信装置から、そのデータ要求情報に対応する暗号化された暗号化対象データ（暗号化データ）を受信し、受信した暗号化データを復号し取得するなどの処理を行う。

【0068】（2） ユーザ鍵生成処理（S100）の詳細動作

図8は、ユーザ鍵生成処理の詳細動作を示すフローチャートである。

【0069】図8に示すように、ユーザ鍵生成処理では、ユーザ鍵生成装置において、ユーザ鍵生成手段により、各ユーザ用に、ユーザ秘密鍵とそのユーザ秘密鍵に対応するユーザ公開鍵を生成し（ステップS110）、ユーザ鍵配送手段により、生成したユーザ秘密鍵を、第三者に盗見しないようにデータ受信装置の秘密鍵保管手段に配送し（ステップS120）、データ受信装置において、ユーザ秘密鍵保管手段によりユーザ秘密鍵を保管し（ステップS130）、また、ユーザ鍵配送手段により、生成したユーザ公開鍵を、第三者に改ざんされないようにデータ送信装置のユーザ公開鍵保管手段に配送し（ステップS140）、データ送信装置において、ユーザ公開鍵保管手段により、ユーザ公開鍵を保管する（ステップS150）。

【0070】ユーザ秘密鍵が第三者に盗見しないように配送するための具体的な手段としては、ユーザ秘密鍵を、ユーザの指定したパスワードを用いて、共通鍵暗号方式で暗号化した後、フロッピーディスクに記録して手渡しで配送するか、ネットワークを介してオンラインで配送するか、または、ICカードを利用して手渡しで配送するなどの手段が利用できる。また、ユーザ公開鍵が、第三者により改ざんされないように配送するための具体的な手段としては、ユーザ公開鍵に、公的な認証局の発行した証明書を添付して転送するか、フロッピーディスクやICカードに記録して手渡しで配送するなどの手段が利用できる。

【0071】（3） データ作成処理（S200）の詳細動作

図9は、データ作成処理の詳細動作を示すフローチャートである。

【0072】図9に示すように、データ作成処理では、暗号化対象データ作成装置において、暗号化対象データ作成手段により、暗号化範囲指定命令や受信者指定命令などを組み込んだ暗号化対象データを作成し(ステップ210)、データ配送手段により、作成した暗号化対象データを、データ送信装置のデータ保管手段に配送し(ステップ220)、データ送信装置において、暗号化対象データを保管する(ステップ220)。

【0073】暗号化対象データを配送するための具体的な実現方法としては、暗号化対象データをフロッピーなどの記録媒体に記録して手渡しで配送するなどの手段が利用できる。

【0074】（4） データ取得処理（S300）の詳細動作

まず、データ送信装置を、WWWサーバとCGIプログラムで、データ受信装置を、WWWブラウザと復号プラグインで構成する場合の詳細動作について説明する。図13は、この場合のデータ取得処理の詳細動作を示すフローチャートである。

【0075】図10に示すように、データ取得処理では、まず、データ受信装置のWWWブラウザにおいて、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り（ステップS310）、データ通信手段により、指定されたデータの送信を要求するデータ要求情報と、オプションとして受信者を指定する受信者識別情報をデータ送信装置に送信し（ステップS320）、データ送信装置のWWWサーバにおいて、データ通信手段により、データ要求情報と受信者識別情報を受信し（ステップS330）、データ取得手段により、受信したデータ要求情報に対応する暗号化対象データを取得し（ステップS340）、データ暗号化手段により、取得された暗号化対象データを、受信者指定命令、もしくは、受信者識別情報で指定された受信者のみが復号できるように暗号化して、暗号化データを作成し（ステップS350）、データ通信手段により、暗号化データをデータ受信装置に送信し（ステップS360）、データ受信装置において、データ通信手段により、暗号化データを受信し（ステップS370）、データ復号手段により、暗号化データを復号し（ステップS380）、データ処理手段により、復号された暗号化データを、ディスプレ表示などのためにデータ出力手段に渡す（ステップS390）。

【0076】ここで、ステップS310においてユーザが取得したいデータを指定する方法としては、URL(Uniform Resource Location)と呼ばれる取得したいデータのアドレス情報（データの保管場所を指定する情報）を直接入力する方法や、取得したいデータのURLを指定する命令の組み込まれたデータにおいて、その命令を実行することによって行う方法などを利用できる。

【0077】また、図11（1）は、データ暗号化手段における暗号化対象データの暗号化（ステップS350）の詳細な動作を示すフローチャートである。

【0078】図11（1）に示すように、データ暗号化手段では、データ鍵生成手段により、データ鍵を生成し

（ステップS351）、共通鍵暗号化手段により、生成したデータ鍵を用いて、暗号化対象データのうち暗号化範囲指定命令で指定された範囲を暗号化し（ステップS352）、公開鍵暗号化手段により、ユーザ公開鍵保管手段に保管されている各ユーザのユーザ公開鍵の中から、受信者指定命令、もしくは、受信者識別情報で指定された受信者のユーザ公開鍵を取得し、取得したユーザ公開鍵を利用して、公開鍵暗号化し（ステップS353）、暗号化データ作成手段により、暗号化されたデータ鍵を指定する暗号鍵情報指定命令と復号範囲指定命令を組み込んだ暗号化データを作成する（ステップS354）。

【0079】また、図11（2）は、データ復号手段における暗号化データの復号（ステップS380）の詳細な動作を示すフローチャートである。

【0080】図11（2）に示すように、データ復号手段では、暗号化データ解析手段により、暗号化データから鍵情報指定命令で指定された暗号化されたデータ鍵を取得し（ステップS381）、公開鍵復号手段により、ユーザ秘密鍵保管手段に保管されたユーザ秘密鍵を用いて、暗号化されたデータ鍵を復号し（ステップS382）、共通鍵復号手段により、復号されたデータ鍵を利用して暗号化データを復号し（ステップS383）、復号された暗号化データを取得する（ステップS384）。

【0081】なお、暗号化対象データに受信者指定命令を組み込むことにより、暗号化対象データの受信者を指定する場合は、データ受信装置からデータ送信装置に受信者識別情報を送信する必要はない。

【0082】次に、データ送信装置を、WWWサーバと暗号化プロキシで、データ受信装置を、WWWブラウザと復号プロキシで構成する場合の詳細動作について説明する。図12は、この場合のデータ取得処理の詳細動作を示すフローチャートである。

【0083】図12に示すように、データ取得処理では、まず、データ受信装置のWWWブラウザにおいて、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り（ステップS410）、データ通信手段により、指定されたデータの送信を要求するデータ要求情報と、オプションとして受信者を指定する受信者識別情報を、データ送信装置に送信し（ステップS420）、データ送信装置のWWWサーバにおいて、データ通信手段により、データ要求情報と受信者識別情報を受信し（ステップS430）、データ取得手段により、受信したデータ要求情報に対応する暗号化対象データを取得し（ステップS440）、データ通信手段により暗号化対象データを暗号化プロキシに送信し（ステップS450）、暗号化プロキシにおいて、データ通信手段により暗号化対象データを受信し（ステップS460）、データ暗号化手段により、取得された暗号化対象データを、受信者指定命令、もしくは、受信者識別情報で指定された受信者のみが復号できるように暗号化して、暗号化データを作成し（ステップS470）、データ通信手段により、暗号化データを復号プロキシに送信し（ステップS480）、データ受信装置の復号プロキシにおいて、データ通信手段により、暗号化データを受信し（ステップS490）、データ復号手段により、暗号化データを復号し（ステップS500）、データ通信手段において、復号された暗号化データをWWWブラウザに送信し（ステップS510）、WWWブラウザのデータ通信手段により、復号された暗号データを受信し（ステップS520）、データ処理手段により、復号された暗号化データを、ディスプレ表示などのためにデータ出力手段に渡す（ステップS530）。

【0084】（実施の形態2）次に、データ送信装置にあらかじめ暗号化データを格納しておき、データ送信装置にて、データ受信装置からの送信要求に対応して、該当の暗号化データをデータ受信装置に送信し、データ受信装置にて、受信した暗号化データを復号して取得する場合について説明する。

【0085】まず、システムの構成について説明し、次に、本システムの詳細な動作について説明する。

【0086】「システムの構成」本実施の形態の全体のシステム構成について説明する。図13は、本実施の形態におけるデータ暗号通信システムの概略構成図である。図13に示すようにデータ暗号通信システムは、データ送信装置1と、データ受信装置2と、これらを接続するネットワーク3と、暗号化データ作成装置6と、ユーザ鍵生成装置5によって構成される。

【0087】ここで、データ受信装置、及び、ユーザ鍵生成装置の構成は、実施の形態1と同じものが利用できるので、ここでは説明を省略する。

【0088】データ送信装置1は、データ受信装置2からのデータ要求情報及びオプションとして受信者識別情報を受信しそのデータ要求情報に対応した暗号化データをデータ受信装置2に送信するためのデータ通信手段11と、上記データ要求情報に対応する暗号化データをデータ保管手段13から取り出し、この暗号化データをデータ通信手段に渡すためのデータ取得手段12と、暗号化データを保管するためのデータ保管手段13で構成される。

【0089】データ送信装置1としては、具体的には、上記データ通信手段と、データ取得手段と、データ保管手段を備えた、既存のWWW(World Wide Web)サーバ（例えば、Netscape Communications社のNetscape Communicationサーバなど）を実装したコンピュータ（パソコンやワークステーションなど）が利用できる。この場合、WWWサーバの備えるデータ通信手段11が、WWWサーバとWWWブラウザ間の標準通信プロトコルであるHTTPプロトコルに基づいてデータ通信を行う。

【0090】暗号化データ作成装置6としては、暗号化対象データを作成する暗号化対象データ作成手段61と、作成した暗号化対象データを暗号化対象データを受信者指定命令にて指定された受信者向けに暗号化して暗号化データを生成するためのデータ暗号化手段62と、暗号化データをデータ送信装置のデータ保管手段13に配送するデータ配送手段63を備えている。データ暗号化手段には、図示していないが鍵生成装置5によって生成された各ユーザのユーザ公開鍵を保管するための公開鍵保管手段を備えている。データ暗号化手段14の詳細構成については実施の形態1の場合と同じであるので説明は省略する。

【0091】暗号化データ作成装置として、具体的には、通常のテキストエディターや既存のWWWデータ（ホームページなど）を作成するための市販のソフトウエア、及び、データ暗号化手段を実現するプログラムとが実装されたコンピュータ（パソコンやワークステーション）が利用できる。

【0092】またデータ配送手段42の具体的な実現方法としては、例えば、暗号化対象データをフロッピーディスクなどの記録媒体に記録してオフラインで配送する手段等をとることができる。

【0093】暗号化対象データ及び暗号化データのデータ構造については、実施の形態1の場合と同じであるので説明を省略する。

【0094】「詳細な動作」次に、本実施の形態の動作について説明する。

【0095】まず、全体の動作概略について説明し、その後、個々の処理の詳細動作について説明する。

【0096】（1） 本実施の形態全体の動作概略

本実施の形態におけるデータ暗号通信システムの全体の動作概略としては、実施の形態1と同様であり、新規のユーザが利用を開始するときに行うユーザ鍵生成処理（ステップS100）と、データの提供者が提供データ（暗号化データ）を作成するときに行う暗号化データ作成処理（ステップS200）と、ユーザが、提供データを取得するときに行うデータ取得処理（ステップS300）からなる。

【0097】ここでユーザ鍵生成処理（S100）は、実施の形態1と同様に、ユーザ自身、もしくは、本システムの管理者が、ユーザ鍵生成装置を利用して行う。具体的には、各ユーザ用のユーザ秘密鍵と、ユーザ秘密鍵に対応するユーザ公開鍵を生成し、生成したユーザ秘密鍵をそのユーザの利用するデータ受信装置に、またユーザ公開鍵を、データ送信装置に配送するなどの処理を行う。

【0098】データ作成処理（S200）は、実施の形態1と異なり、データ提供者が、暗号化データ作成装置を利用して行う。

【0099】具体的には、暗号化対象データを作成し、作成した暗号化対象データを暗号化し、データ送信装置に配送するなどの処理を行う。

【0100】データ取得処理（S300）は、実施の形態1と異なり、各ユーザが、データ受信装置を利用して行う。具体的には、各ユーザが、自分のデータ受信装置を利用して、取得したい提供データ（暗号化データ）の送信を要求するデータ要求情報をデータ送信装置に送信し、データ送信装置から、そのデータ要求情報に対応する暗号化データを受信し、受信した暗号化データを復号し取得するなどの処理を行う。

【0101】（2） ユーザ鍵生成処理（S100）の詳細動作

ユーザ鍵生成処理の動作は、実施の形態1の場合と同じであるので説明は省略する。

【0102】（3） データ作成処理（S200）の詳細動作

図14は、データ作成処理の詳細動作を示すフローチャートである。

【0103】図14に示すように、データ作成処理では、暗号化データ作成装置において、暗号化対象データ作成手段により、暗号化範囲指定命令や受信者指定命令などを組み込んだ暗号化対象データを作成し(ステップ210)、暗号化対象データを、受信者指定命令で指定された受信者のみが復号できるように暗号化して、暗号化データを作成し(ステップ220)、データ配送手段により、作成した暗号化対象データを、データ送信装置のデータ保管手段に配送し(ステップ230)、データ送信装置において、暗号化データを保管する(ステップ240)。

【0104】データ暗号化手段における暗号化対象データの暗号化（ステップS220）の詳細な動作は実施の形態1の場合と同様であるので説明は省略する。

【0105】暗号化データを配送するための具体的な実現方法としては、暗号化データをフロッピーなどの記録媒体に記録して手渡しで配送する方法や、ネットワークを利用してオンラインで配送するなどの手段が利用できる。

【0106】（4） データ取得処理（S300）の詳細動作

まず、データ受信装置を、WWWブラウザと復号プラグインで構成する場合の詳細動作について説明する。図15は、この場合のデータ取得処理の詳細動作を示すフローチャートである。

【0107】図15に示すように、データ取得処理では、まず、データ受信装置のWWWブラウザにおいて、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り（ステップS310）、データ通信手段により、指定されたデータの送信を要求するデータ要求情報を送信し（ステップS320）、データ送信装置のWWWサーバにおいて、データ通信手段により、データ要求

情報と受信者識別情報を受信し（ステップS330）、データ取得手段により、受信したデータ要求情報に対応する暗号化データを取得し（ステップS340）、データ通信手段により、暗号化データをデータ受信装置に送信し（ステップS350）、データ受信装置において、データ通信手段により、暗号化データを受信し（ステップS360）、データ復号手段により、暗号化データを復号し（ステップS370）、データ処理手段により、復号された暗号化データを、ディスプレ表示などのためにデータ出力手段に渡す（ステップS380）。

【0108】データ復号手段における暗号化データの復号（ステップS370）の詳細な動作は実施の形態1の場合と同様であるので説明は省略する。

【0109】次に、データ受信装置を、WWWブラウザと復号プロキシで構成する場合の詳細動作について説明する。図16は、この場合のデータ取得処理の詳細動作を示すフローチャートである。

【0110】図16に示すように、データ取得処理では、まず、データ受信装置のWWWブラウザにおいて、ユーザ入力手段により、ユーザから取得したいデータの指定を受け取り（ステップS410）、データ通信手段により、指定されたデータの送信を要求するデータ要求情報を、データ送信装置に送信し（ステップS420）、データ送信装置のWWWサーバにおいて、データ通信手段により、データ要求情報と受信者識別情報を受信し（ステップS430）、データ取得手段により、受信したデータ要求情報に対応する暗号化データを取得し（ステップS440）、データ通信手段により暗号化データを復号プロキシに送信し（ステップS450）、データ受信装置の復号プロキシにおいて、データ通信手段により、暗号化データを受信し（ステップS460）、データ復号手段により、暗号化データを復号し（ステップS470）、データ通信手段において、復号された暗号化データをWWWブラウザに送信し（ステップS480）、WWWブラウザのデータ通信手段により、復号された暗号データを受信し（ステップS490）、データ処理手段により、復号された暗号化データを、ディスプレ表示などのためにデータ出力手段に渡す（ステップS500）。

【0111】なお、実施の形態1、及び、実施の形態2では、データの送信及びデータの受信に、WWWサーバ及びWWWを利用する場合について説明したがそれに限るものではない。

【0112】また、データとして、HTML言語に基づいて各種データ処理の命令が組み込まれたデータの場合について説明したが、それに限るものではない。

【0113】また、データの暗号化手段として、データの暗号化に共通鍵暗号方式を利用し、データの暗号化に利用したデータ鍵の暗号化に公開鍵暗号方式を利用する場合について説明したが、それに限るものではない。

【0114】

【発明の効果】本発明によれば、暗号化対象データに、暗号化する範囲を指定する暗号化範囲指定命令を組み込むことにより、暗号化対象データは、暗号化範囲指定命令で指定された範囲のみ暗号化される。このため、必要に応じて、暗号化対象データの重要な部分のみを暗号化したり、一部はすべての受信者に視聴させることが可能となる。

【0115】また、暗号化対象データに、受信者を指定する受信者指定命令を組み込むことにより、暗号化対象データを、指定した受信者以外は復号できないように暗号化することが可能となる。すなわち、必要に応じて、あらかじめ受信者を限定することが可能となる。

【0116】また、特に、データ送信装置を、WWWサーバと、暗号化対象データのうち暗号化範囲指定命令で指定された範囲のみを暗号化するためのデータ暗号化手段とWWWサーバ及びWWWブラウザとの間でデータの送受信を行うためのデータ通信手段とを備えた暗号化プログラムとを実装したコンピュータで構成することにより、既存のWWWサーバを変更することなく利用した、データの暗号送信を行うデータ暗号装置が提供可能となる。

【0117】同様に、特に、データ復号装置を、WWWブラウザと、暗号化データのうち復号範囲指定命令で指定された範囲のみを復号するデータ復号手段とWWWサーバ及びWWWブラウザとの間でデータの送受信を行うデータ通信手段とを備えた復号プログラムとを、実装したコンピュータで構成することにより、既存のWWWブラウザを変更することなく利用した、暗号化データの復号受信を行うデータ暗号装置が提供可能となる。

【0118】また、特に、HTML言語のコメント命令を利用して暗号処理命令を定義するため、既存のWWWサーバやブラウザに影響を与えることがない。

【図面の簡単な説明】

【図1】本発明の実施の形態1のデータ暗号通信システムの全体構成図

【図2】データ送信装置及びデータ受信装置の構成図

【図3】暗号化プロキシ及び復号プロキシを利用したデータ暗号通信システムの全体構成図

【図4】データ暗号化手段及びデータ復号手段の詳細構成図

【図5】暗号化対象データ及び暗号化データのデータ構造例を示す図

【図6】暗号処理命令の一覧を示す図

【図7】全体の動作概略を示すフローチャート

【図8】ユーザ鍵生成処理のフローチャート

【図9】データ作成処理のフローチャート

【図10】データ取得処理のフローチャート

【図11】データ暗号化手段及びデータ復号手段の処理のフローチャート

【図12】暗号化プロキシ及び復号プロキシ利用時のデータ取得処理のフローチャート

【図13】本発明の実施の形態2のデータ暗号通信システムの全体構成図

【図14】データ作成処理のフローチャート

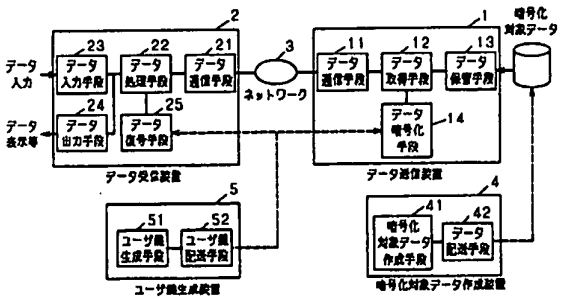
【図15】データ取得処理のフローチャート

【図16】復号プロキシ利用時のデータ取得処理のフローチャート

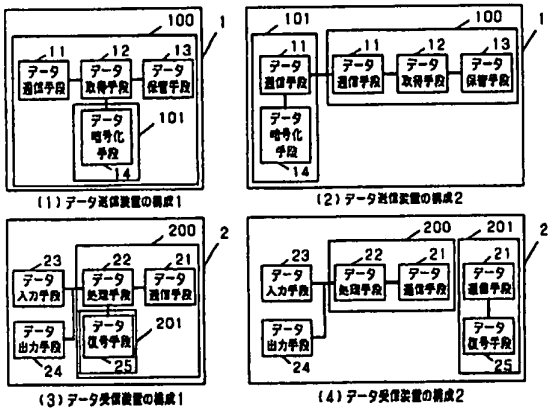
【符号の説明】

1　データ送信装置
2　データ受信装置
4　暗号化対象データ作成装置
5　ユーザ鍵生成装置
14　データ暗号化手段
25　データ復号手段
101　暗号プロキシ
200　WWWブラウザ
201　復号プロキシ

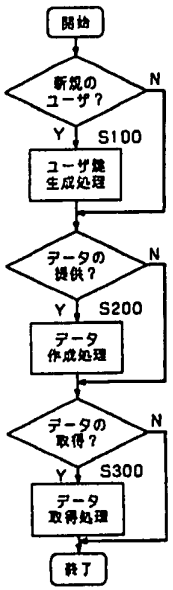
【図1】



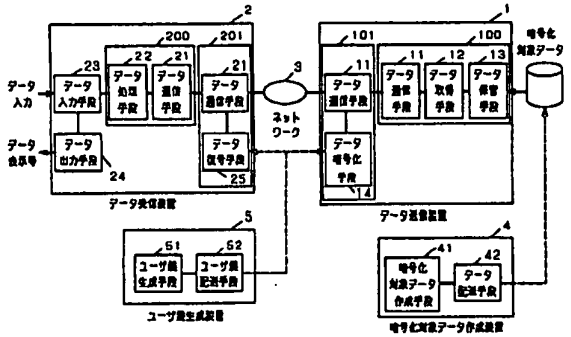
【図2】



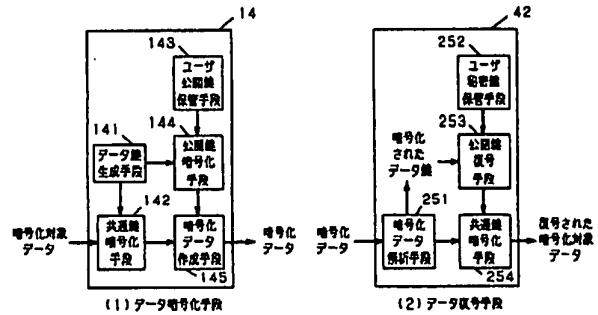
【図7】



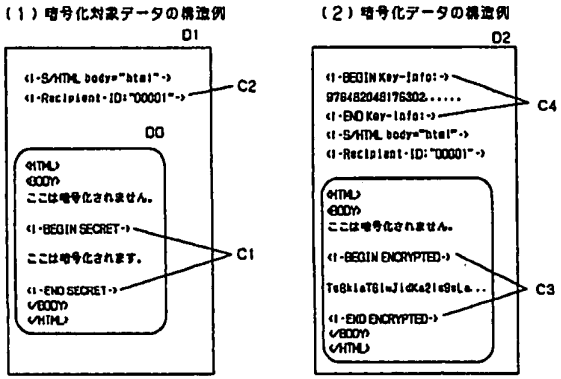
【図3】



【図4】



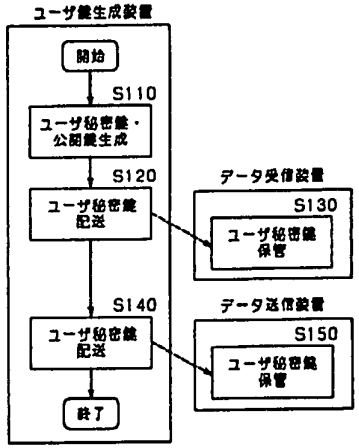
【図5】



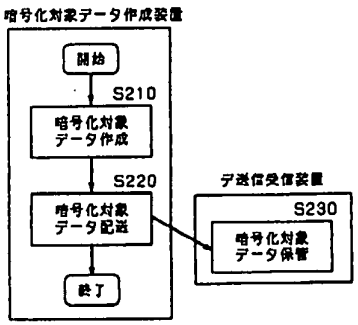
【図6】

命令	指定方法
暗号化範囲指定命令	暗号化する範囲の開始を<!-BEGIN SECRET->で指定し終了を<!-END SECRET->で指定する
受信者指定命令	受信者の識別番号を以下のように指定する <!-Recipient-ID:"00001"->
復号範囲指定命令	復号する範囲の開始を<!-BEGIN ENCRYPTED->で指定し終了を<!-END ENCRYPTED->で指定する
鍵情報指定命令	鍵情報を以下のように指定する。 <!-BEGIN Key-Info:-> 9784820481763O2. <!-END Key-Info:->

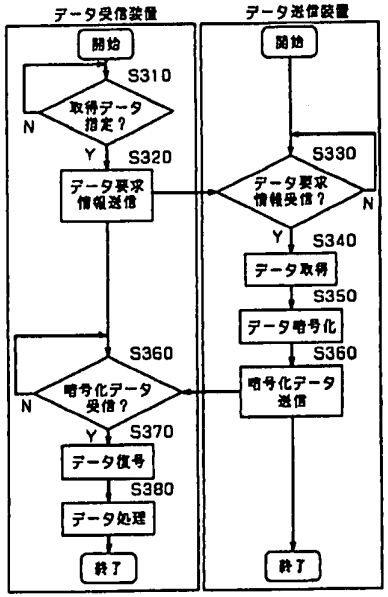
【図8】



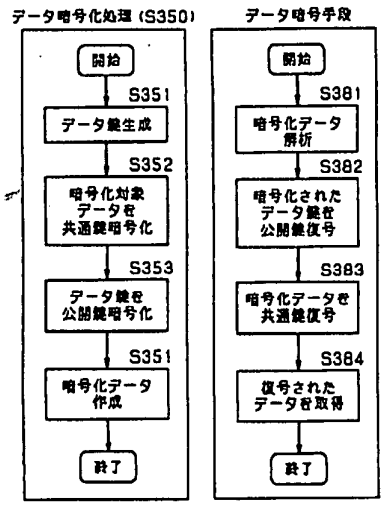
【図9】



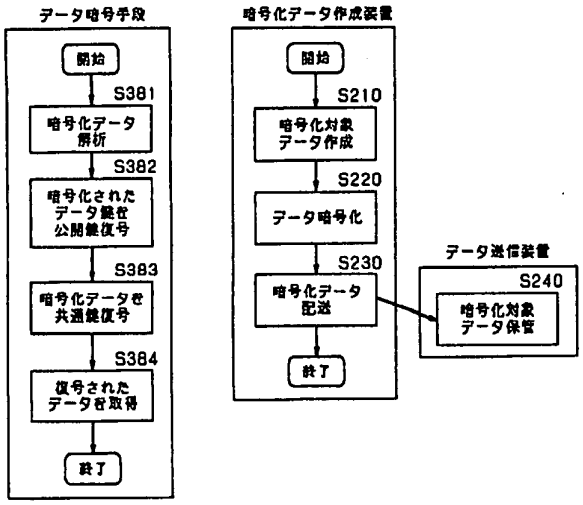
【図10】



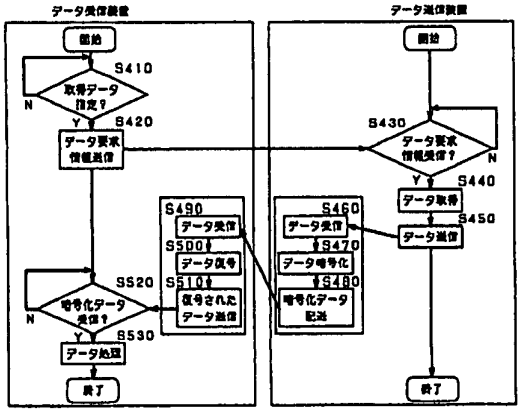
【図11】



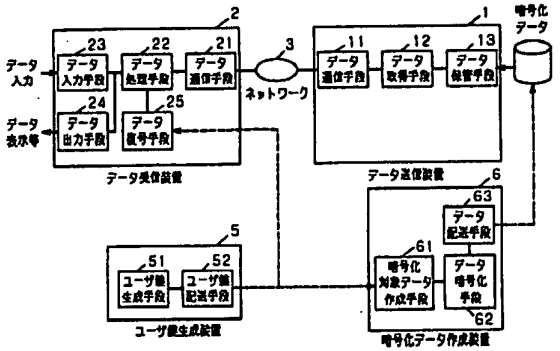
【図14】



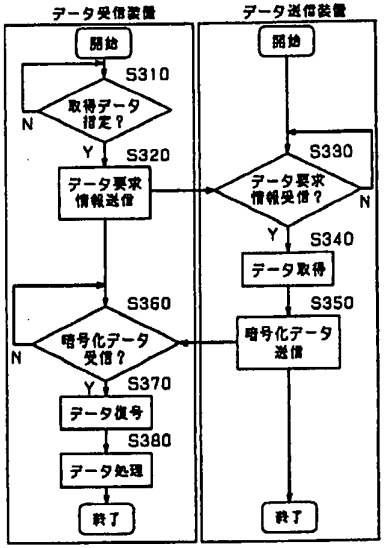
【図12】



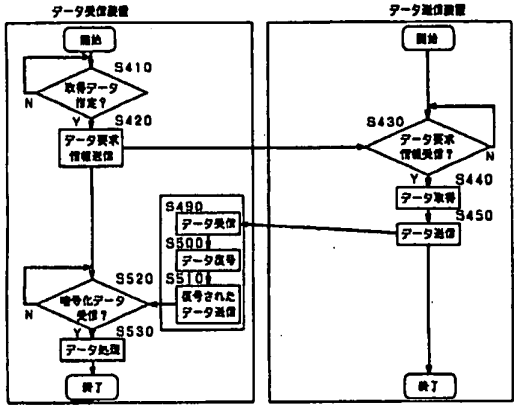
【図13】



【図15】



【図１６】



フロントページの続き

(72)発明者　西條　猛
愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内

(72)発明者　小野　貴敏
愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階　株式会社松下電器情報システム名古屋研究所内